Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2014–2015

34 034 Implementatie van de richtlijn 2013/40/EU van het Europees parlement en de Raad over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad (PbEU L 218/8)

Nr. 5

NOTA NAAR AANLEIDING VAN HET VERSLAG

Ontvangen 11 februari 2015

1. Inleiding

Met belangstelling heb ik kennisgenomen van het verslag dat de vaste commissie voor Veiligheid en Justitie over dit wetsvoorstel heeft uitgebracht. Het verheugt mij dat de leden van de VVD-fractie konden onderschrijven dat de strafbaarstellingen van computercriminaliteit worden aangescherpt en dat strafverzwarende omstandigheden worden toegevoegd. Met deze leden ben ik van mening dat het, gelet op de impact van cybercrime en het belang van burgers, bedrijven en overheden bij een veilige en betrouwbare digitale en vitale infrastructuur, van groot belang is dat er een duidelijk signaal wordt afgegeven, dat een stevige aanpak mogelijk wordt gemaakt en dat het daarbij noodzakelijk en onvermijdelijk is dat wordt aangesloten bij de internationale ontwikkelingen en bij de bestaande wetgeving.

Deze leden merkten op dat in de memorie van toelichting wordt gesproken over voorschriften om informatie uit te wisselen en een 24/7-netwerk van contacten. Zij vroegen welke organisaties hierbij vanuit Nederland betrokken zijn en wat de onderlinge verhoudingen zijn. In het bijzonder vroegen zij of het departement met het Nationaal Cyber Security Centrum (NCSC) de regie heeft en eindverantwoordelijk is. Zij vroegen verder hoe de samenwerking met de private sector verloopt en wat in Nederland de rol is van de onlangs in Den Haag gevestigde cybereenheid van de NAVO.

Artikel 13 van de richtlijn bepaalt dat de lidstaten ervoor zorgen dat zij over een operationeel nationaal contactpunt voor de informatie-uitwisseling over de in de richtlijn bedoelde strafbare feiten beschikken en gebruikmaken van het bestaande netwerk van operationele contactpunten die vierentwintig uur per dag en zeven dagen per week bereikbaar zijn (het 24/7-netwerk). De bepaling verwijst naar het 24/7-netwerk zoals dat reeds moest worden ingesteld op grond van artikel 35 van het Cybercrimeverdrag. Per land is een contactpunt beschikbaar om te voorzien in onmiddellijke bijstand bij verzoeken uit andere landen tot ondersteuning en rechtshulp bij aangelegenheden inzake computercriminaliteit. In Nederland is het Team High Tech Crime (THTC) van de Dienst Nationale

kst-34034-5
ISSN 0921 - 7371
’s-Gravenhage 2015

Recherche van de Landelijke Eenheid van de Nationale Politie aangewezen als contactpunt. Het gezag berust bij de coördinerend officier van justitie die is geplaatst bij het Landelijk Parket van het openbaar ministerie. Hier berust de eindverantwoordelijkheid.
Het NCSC – dat nauw samenwerkt met de vitale private sectoren (publiek-private samenwerking (PPS)) – heeft een andere rol. Het NCSC, dat valt onder de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) beschikt over expertise en advies om proactief bij te dragen aan preventie (bewustwording en bescherming) en preparatie ten aanzien van cybersecurity. Daarnaast adviseert en biedt het NCSC anderszins ondersteuning aan onderdelen van de rijksoverheid en vitale private organisaties bij dreigingen en incidenten en speelt het NCSC een rol in de operationele coördinatie bij een ICT-crisis. Het werkt voor de vervulling van zijn taken ook internationaal samen via het International Watch and Warning Network (IWWN), een wereldwijd netwerk van overheidsvertegenwoordigers uit vijftien landen op het gebied van beleid en operationele uitvoering ingeval van een internationaal ICT-incident.
Het in Den Haag gevestigde NAVO Communicatie en Informatie Agentschap (NCIA), waar deze leden naar verwezen, is gericht op onderzoek en innovatie voor de NAVO, onder meer op het gebied van informatietechnologie, cybersecurity en raketafweer. De opdracht van dit agentschap is niet vergelijkbaar met het operationele doel van het THTC bij de aanpak van computercriminaliteit.

De leden van de PvdA-fractie gaven aan met belangstelling kennis te hebben genomen van het wetsvoorstel. Zij gaven verder aan zich bewust te zijn van de grote gevolgen van een aanval op computersystemen die vitale onderdelen van de economie sturen en de maatschappelijke ontwrichting die dit tot gevolg kan hebben. Hiertoe is strenge en heldere wetgeving nodig, aldus deze leden.
De leden van deze fractie merkten op dat het openbaar ministerie (OM) in zijn advies pleit voor één titel in het Wetboek van Strafrecht (WvSr) waarin alle strafbepalingen ten aanzien van computercriminaliteit worden opgenomen.
In antwoord op de vraag van deze leden daarnaar, wil ik graag vooropstellen dat opnemen van een dergelijke afzonderlijke titel het bestek van dit wetsvoorstel, dat enkel ziet op de implementatie van een richtlijn, te buiten gaat. Los hiervan, merk ik graag het volgende over het voorstel – waarvan ik met belangstelling kennisgenomen heb – op. Als de kern van een strafbaar feit wordt veelal een bepaalde gedraging gezien. Voor de huidige plaatsing pleit dan ook dat is aangesloten bij de gepleegde gedraging. Zo is de strafbaarstelling van vernieling en beschadiging van computergegevens (artikel 350a Sr) opgenomen bij de overige bepalingen over vernieling en beschadiging. Daarbij komt dat er geen heldere afbakening is te geven van de delicten die als «computerdelict» moeten worden aangemerkt. In de eerste plaats omdat de meeste thans in het spraakgebruik wel als computerdelicten aangemerkte strafbare feiten een breder bereik hebben dan computers alleen. Zo hebben de artikelen 161sexies en 350a WvSr niet alleen betrekking op computers (geautomatiseerde werken), maar ook op werken voor telecommunicatie. Bovendien geldt dat, door de maatschappelijke en technologische ontwikkelingen, ook steeds meer klassieke strafbare feiten denkbaar zijn ten aanzien van computers en computergegevens of worden gepleegd via de computer of door manipulatie van computergegevens. Ik noem als voorbeelden de valsheidsdelicten, belediging, afpersing en bedrog (oplichting).
Een aparte titel in het wetboek voor computerdelicten zou betekenen dat steeds naast de generieke strafbepaling, een bijzondere strafbaarstelling moet worden opgenomen voor zover het delict is gepleegd tegen of met een computer of computergegevens. Dit acht ik minder wenselijk gelet op de systematiek van ons Wetboek van Strafrecht. Die systematiek bestaat

eruit dat zoveel mogelijk wordt gewerkt met generieke strafbepalingen waaronder verschillende feitencomplexen kunnen worden gebracht.

Met de leden van de PvdA-fractie, zo beantwoord ik een volgende vraag, ben ik van mening dat het voor de aanpak van computercriminaliteit van groot belang is dat alle EU-lidstaten de EU-richtlijnen en EU-verdragen uitvoeren. In verband met de naar zijn aard veelal grensoverschrijdende gevolgen is een gezamenlijke Europese aanpak noodzakelijk.

Deze leden vroegen welke lidstaten het EU-kaderbesluit 2005/222/JBZ hebben ondertekend en welke niet en wat daarvoor de reden is. Zij vroegen of deze lidstaten nu wel aangesloten zijn bij deze richtlijn. Kaderbesluiten worden vastgesteld door de Raad van Ministers. Alle lidstaten van destijds waren gehouden dit kaderbesluit te implementeren. Blijkens het rapport uit 2008 van de Europese Commissie over de implementatie van het kaderbesluit, waren de bepalingen uit het kaderbesluit over het algemeen adequaat door de lidstaten geïmplementeerd. Ik verwijs naar het verslag van de Commissie aan de Raad op basis van artikel 12 van het kaderbesluit van de Raad van 24 februari 2005 over aanvallen op informatiesystemen (COM(2008)448) en het explanatory memorandum gevoegd bij het richtlijnvoorstel (COM(2010)517), blz. 2 en 4.

De leden van deze fractie wezen verder op het Aanvullend Protocol bij het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, betreffende de strafbaarstelling van handelingen van racistische en xenofobische aard verricht via computersystemen (Trb. 2003, 60 en Trb. 2005, 46). Zij merkten op dat slechts een beperkt aantal landen van buiten Europa bij dit Protocol zijn aangesloten en vroegen welk signaal hiervan uitgaat. Zij vroegen hoe computercriminaliteit bestreden kan worden als niet alle landen hiertoe samenwerken. Graag beantwoord ik deze vragen in onderlinge samenhang als volgt.

Het genoemde Aanvullend Protocol hoort bij het zogenoemde Cybercrimeverdrag (Trb. 2002, 18 en Trb. 2004, 290) van de Raad van Europa. Het Cybercrimeverdrag van de Raad van Europa, is naast door Europese Staten, door Australië, Japan, de Verenigde Staten, de Dominicaanse republiek, Panama en Mauritius geratificeerd. Zuid-Afrika heeft het verdrag ondertekend. Verder zijn Argentinië, Chili, Costa Rica, de Filipijnen, Israël, Marokko, Mexico, Senegal, Sri Lanka en Tonga uitgenodigd om toe te treden tot het verdrag. Deze landen zijn bezig met de toetredingsprocedure. Het Cybercrimeverdrag is op het gebied van computercriminaliteit het meest wijdverbreide internationale rechtsinstrument. Het fungeert daarnaast voor veel landen als «model law».

In een zogenoemde «open ended working group» van VN-landen over de aanpak van cybercrime, is onder meer gesproken over de vraag naar de wenselijkheid van een rechtsinstrument op globaal niveau. Ten behoeve van de beraadslagingen over dit onderwerp is een conceptrapport opgesteld (conceptrapport uit 2013 van de United Nations Office on Drugs and Crime (UNODC) «Comprehensive study on Cybercrime»). De werkgroep is tot op heden twee keer bijeengeweest. De landen konden tijdens deze bijeenkomsten geen consensus bereiken over de aan het onderzoek te verbinden conclusies. Vooralsnog, en in afwachting van een mogelijke nieuwe bijeenkomst van de werkgroep, heeft de meerderheid van landen het UNODC opgeroepen zoveel mogelijk initiatieven te ontplooien rondom capaciteitsopbouw in verschillende landen om een effectieve aanpak van computercriminaliteit te vergroten. Ook vanuit de Raad van Europa is er via zogenoemde capaciteitsopbouwprojecten contact met verschillende landen die het Cybercrimeverdrag als modelrecht willen gebruiken of ondersteuning willen bij het inrichten, opbouwen en laten functioneren van rechtshandhavingsdiensten en rechtspleging. Evenals andere lidstaten van de Europese Unie, is Nederland van mening dat het Cybercrimeverdrag het juridisch vertrekpunt moet zijn bij de aanpak van computercriminaliteit, zowel

binnen de Unie als in de samenwerking met andere landen (zie de conclusies van de Raad van Ministers over de EU Cybersecurity Strategy van 22 juli 2013, nr. 12109/13).

De regels opgenomen in het Cybercrimeverdrag over de internationale samenwerking voor uitwisseling van, of toegang tot data sluiten aan bij de heersende opvattingen en gewoonten van het internationale recht, zo beantwoord ik de vraag van deze leden of er een groot verschil van mening is tussen de landen die bij het protocol zijn aangesloten en andere landen over hoe omgegaan wordt met data in het algemeen.

De leden van de PvdA-fractie stelden voorts enkele vragen over de verstrekking van statistische gegevens, waarover in de richtlijn bepalingen zijn opgenomen, in het bijzonder in relatie tot het THTC.

Artikel 14 van de richtlijn, zo beantwoord ik deze vragen, verplicht ertoe om te zorgen voor een systeem voor het registreren, aanmaken en verstrekken van statistische gegevens over de in de artikelen 3 tot en met 7 van de richtlijn bedoelde strafbare feiten. Daarbij moeten ten minste de reeds beschikbare gegevens over het aantal strafbare feiten worden geregistreerd en het aantal personen dat is vervolgd en veroordeeld. Deze gegevens moeten worden verstrekt aan de Europese Commissie. Die zorgt ervoor dat er een geconsolideerd overzicht van de statistische verslagen wordt gepubliceerd en aan de bevoegde gespecialiseerde agentschappen en organen van de Unie wordt gezonden. Bij dit laatste kan gedacht worden aan Europol. De gegevens worden aan hen ter beschikking gesteld naar gelang hun taken en informatiebehoeften, opdat er een vollediger beeld ontstaat van de problematiek rondom computercriminaliteit en netwerk- en informatiebeveiliging op het niveau van de Unie en er een doeltreffender reactie kan worden geformuleerd. Het verstrekken van informatie kan een beter inzicht bevorderen in huidige en toekomstige bedreigingen, en aldus bijdragen tot een meer passende en gerichte besluitvorming over het bestrijden en voorkomen van aanvallen op informatiesystemen (vgl. overweging 24 van de richtlijn).

Het ligt voor de hand dat dergelijke gegevens in eerste instantie worden aangeleverd door het THTC, maar mogelijk ook door bijvoorbeeld het openbaar ministerie dat – zoals hierboven aan de orde kwam – ook een rol heeft bij de bestrijding van computercriminaliteit. Ten aanzien van de vraag van deze leden naar de inhoud en de frequentie van de te verstrekken gegevens door andere lidstaten, merk ik op dat op dit moment de verplichting tot het verstrekken van gegevens nog niet bestaat. Ten behoeve van de verdere implementatie van de richtlijn zullen nadere afspraken worden gemaakt over de registratie en verstrekking van de gegevens. Hierover wordt gesproken met de Europese Commissie en andere lidstaten.

De leden van de SP-fractie hadden met belangstelling kennisgenomen van het wetsvoorstel. Zij vroegen of politie en justitie knelpunten ervaren doordat de verschillende strafbare feiten aangaande computercriminaliteit verspreid over het WvSr staan en of de regering het wenselijk acht om tot een afzonderlijke titel te komen.

Het openbaar ministerie, zo beantwoord ik de vragen van deze leden, heeft in het advies bij dit wetsvoorstel geadviseerd om bij een daarvoor geschikte gelegenheid alle strafbepalingen die betrekking hebben op computercriminaliteit in één titel te plaatsen. Hieraan bestaat, aldus dat advies, in de praktijk behoefte, omdat die strafbepalingen dan beter in onderlinge samenhang kunnen worden toegepast. Zoals ik hierboven in antwoord op een vraag van de leden van de PvdA-fractie reeds aangaf, heb ik met belangstelling kennisgenomen van dit advies. Na een nadere afweging kom ik evenwel tot de conclusie dat een afzonderlijke titel met computerdelicten leidt tot afbakeningsproblemen – zeker nu ook steeds meer «klassieke» delicten tegen of met computers of computergegevens kunnen worden gepleegd – en niet in lijn zou zijn met de systematiek van

het Wetboek van Strafrecht. Voor een uitgebreidere toelichting verwijs ik deze leden kortheidshalve naar mijn hierboven gegeven antwoord op de vraag van de leden van de PvdA-fractie.
Het antwoord op de vraag van deze leden in hoeverre naast het Wetboek van Strafvordering ook het Wetboek van Strafrecht gemoderniseerd zal worden, luidt dat de modernisering van het Wetboek van Strafvordering op dit moment prioriteit heeft. Het betreft een majeure wetgevingsoperatie, waarvoor veel wetgevingscapaciteit en inspanningen van alle (keten)partners nodig zijn. Gelet op alle inspanningen gericht op de modernisering van het Wetboek van Strafvordering en de gevolgen daarvan voor de praktijk, is een algehele modernisering van het Wetboek van Strafrecht thans niet aan de orde. Uiteraard zullen, daar waar dat noodzakelijk is, wetsvoorstellen worden ingediend waarin strafbepalingen gemoderniseerd en aangepast worden.

De leden van de PVV-fractie gaven aan kennis te hebben genomen van het wetsvoorstel en daarbij nog enkele vragen te hebben. Graag beantwoord ik de door hen gestelde vragen in het navolgende.

De leden van de CDA-fractie hadden met belangstelling kennisgenomen van het wetsvoorstel. Zij hadden daarover nog enkele vragen.
De leden van deze fractie stelden enkele vragen over de omvang van en schade als gevolg van cyberaanvallen en computercriminaliteit in de afgelopen jaren en de omvang van de opsporingsactiviteiten daaromtrent. Graag beantwoord ik deze vragen als volgt.
Helaas zijn de specifieke cijfers over strafrechtelijke opsporingsonderzoeken waar deze leden naar vroegen, niet beschikbaar. Door de wijze waarop de diverse systemen bij het openbaar ministerie en de politie zijn ingericht voor hun eigen bedrijfsvoering en verslaglegging, zijn die systemen niet ingericht om de gegevens zoals door deze leden gevraagd, te genereren. De vraag van deze leden wat de jaarlijks geschatte maatschappelijke schade is als gevolg van cybercrime kan ik helaas evenmin beantwoorden. De diverse cijfers die wereldwijd worden gepubliceerd, lopen ver uiteen. Verder moet worden bedacht dat computercriminaliteit een grensoverschrijdend karakter heeft, waarbij de bij de rechtshandhaving in het algemeen geldende randvoorwaarde dat er een goed vast te stellen (veelal territoriale band) is tussen verdachte, pleegplaats, slachtoffer en plaats van slachtofferschap, veelal niet aanwezig is. Opsporingsonderzoeken vinden daardoor niet altijd (alleen) in Nederland plaats. Hetzelfde geldt voor vervolging en berechting. Dit zal een van de aandachtspunten zijn bij het eerdergenoemde overleg met de Europese Commissie en andere lidstaten over de op basis van de richtlijn te genereren statistieken. Wel kan ik verwijzen naar de zogenoemde Veiligheidsmonitor die sinds 2012 jaarlijks door het Centraal Bureau voor de Statistieken (CBS) wordt gepubliceerd. In de Veiligheidsmonitor van 2013 gaf ruim één op de acht personen van vijftien jaar of ouder aan in de daaraan voorafgaande twaalf maanden slachtoffer te zijn geworden van computercriminaliteit; twaalf procent van de personen van vijftien of ouder werd geconfronteerd met een of meer vormen van computercriminaliteit. De helft van hen was het slachtoffer van hacken (inbraak op computer, smartphone, e-mailaccount of website). Een kwart van deze personen werd gepest via internet en een kwart had te maken met aan- of verkoopfraude. Een klein deel van de respondenten was slachtoffer van identiteitsfraude (gebruik van persoonsgegevens voor financieel gewin). Jongeren – zo blijkt uit de monitor –, die relatief actief zijn op internet, hebben vaker te maken met computercriminaliteit. Bijna één op de vijf jongeren tussen de vijftien en vijfentwintig jaar werd slachtoffer van computercriminaliteit. Ook bij de vijftentwintig- tot vijfenveertigjarigen is het aantal slachtoffers, met vijftien procent, hoger dan gemiddeld. Dit beeld komt overeen met het in 2013 gepubliceerde onderzoek van de NHL

Hogeschool en de Politieacademie naar computercriminaliteit (M.M.L. Domenie, E.R. Leukfeldt, J.A. van Wilsem, J. Jansen en W. Ph. Stol «Slachtofferschap in een gedigitaliseerde samenleving»; Een onderzoek onder burgers naar e-fraude, hacken en ander veel voorkomende criminaliteit, Boom Lemma, 2013). Blijkens dit onderzoek is computercriminaliteit een veelvoorkomend probleem. Het onderzoek schetst de snelle digitalisering van onze maatschappij en hoe die doordringt in de criminaliteit. Er zijn niet alleen «nieuwe» vormen van criminaliteit bij gekomen, maar ook klassieke delicten als bedreiging en oplichting vinden tegenwoordig plaats met behulp van internet.
Met betrekking tot (bekende) grootschalige cyberaanvallen, waarnaar deze leden vroegen, verwijs ik graag naar het cybersecuritybeeld dat jaarlijks door het Ministerie van Veiligheid en Justitie wordt gepubliceerd. Het cybersecuritybeeld geeft een beeld van de ontwikkelingen en dreigingen in het digitale domein in de voorgaande twaalf maanden. In 2014 is het vierde Cybersecurity Beeld Nederland (CSBN-4) gepubliceerd. Onderdeel hiervan is een rapportage van het aantal bij het NCSC geregistreerde incidenten. In 2014 was het NCSC betrokken bij in totaal 713 incidenten. Het is van belang om hierbij aan te merken dat het gaat om vrijwillig gemelde incidenten van partijen binnen de rijksoverheid en de vitale sectoren. Vermelding verdient dat inmiddels een wetsvoorstel voor consultatie is verzonden dat mede is opgesteld naar aanleiding van de motie-Hennis-Plasschaert c.s. inzake het verplicht melden van bepaalde ICT-inbreuken (de zogenoemde security breach notification); zie Kamerstukken II 2011/12, 26 643, nr. 202.
Niet alle bij de NCSC gemelde incidenten zijn te kwalificeren als grootschalige cyberaanvallen. Het gaat ook om bijvoorbeeld meldingen inzake gedetecteerde virussen. De incidenten kunnen zich op verschillende manieren manifesteren, bijvoorbeeld als aanvallen gericht op informatie, zoals in het geval van digitale spionage, of gericht op diefstal of manipulatie van informatie. Ook zijn er incidenten waarbij sprake is van een aanval gericht op ICT, de verstoring van ICT of de overname van ICT. Bij omvangrijke incidenten of incidenten met aanzienlijke impact in de afgelopen jaren, zoals bij de DDoS-aanvallen in het voorjaar van 2013, de KPN-hack in 2012 en het DigiNotar incident in 2011, is de Kamer hierover specifiek geïnformeerd.
De voornemens inzake de opsporing van computercriminaliteit, waarnaar deze leden verwijzen, zijn onderdeel van de Veiligheidsagenda en maken onderdeel uit van de landelijke prioriteiten. Naast de bestrijding van computercriminaliteit, zijn er nog andere landelijke prioriteiten, zoals de bestrijding van kinderpornografie en kindersekstoerisme. Ten aanzien van computercriminaliteit is binnen de opsporing en vervolging behoefte aan bijzondere expertise. Deze expertise is nog schaars binnen de opsporing in de regionale eenheden. De verwachting is dat de politie in staat zal zijn om in 2015 de in de Veiligheidsagenda vermelde vijfentwintig complexe onderzoeken voor haar rekening te nemen. De komende jaren is het de bedoeling om de beschikbare expertise binnen de politie te vergroten en zal ook de productie verder omhoog gaan. Binnen deze randvoorwaarden doet het voornemen dus recht aan de omvang van de problematiek.
Deze leden vroegen voorts hoeveel fte de afgelopen twee jaar beschikbaar waren en de aankomende twee jaar beschikbaar zijn voor het THTC. Ook vroegen zij een overzicht van het aantal officieren van justitie dat zich specifiek richt op de vervolging van computerdelicten.
Het THTC is in drie tranches uitgebreid. De eerste uitbreiding vond plaats in 2012 en de tweede uitbreiding werd eind 2013 afgerond. Eind 2014 is de derde en laatste tranche medewerkers ingestroomd. Daarmee is de capaciteitsuitbreiding van het THTC naar honderdnegentien fte voltooid (met uitzondering van enkele vacatures door door- en uitstroom). Het team dat zich bezighoudt met high tech crime bij het Landelijk parket van het openbaar ministerie is in 2014 uitgebreid van vier maar zeven fte. Al

langere tijd heeft ieder parket de beschikking over een gespecialiseerde «cyberofficier» en parketsecretaris; zie het jaarbericht van het openbaar ministerie over 2013.
In antwoord op de vraag van deze leden naar het aantal keer per jaar dat een DigiD geblokkeerd wordt, wil ik graag vooropstellen dat het blokkeren van een DigiD niet het gevolg is van aanvallen op informatiesystemen, maar wordt toegepast in het geval van misbruik van een DigiD of als het gevaar bestaat van mogelijk misbruik. Het is lastig om een gemiddelde te geven van het aantal malen dat een DigiD per jaar geblokkeerd wordt. Cijfers kunnen in een bepaalde periode sterk fluctueren. Zo heeft de Minister van Binnenlandse Zaken en Koninkrijksrelaties Uw Kamer bij brief van 16 oktober 2014 bericht over een specifieke fraudezaak waarin 5000 DigiD's zijn verwijderd.
Naar aanleiding van enkele DDoS-aanvallen op DigiD zijn aanvullende maatregelen getroffen om dergelijke aanvallen af te slaan. Deze maatregelen zijn tot op heden effectief gebleken. Dit heeft mede geleid tot de beschikbaarheid van DigiD volgens de afgesproken normen.
Voorts stelden deze leden enkele vragen over DigiD bij de gemeenten, die ik graag als volgt beantwoord.
In september 2014 is bij Logius, de beheerder van DigiD, melding gemaakt van een kwetsbaarheid in hun ConsentManagementSysteem (CMS). Na onderzoek van Logius bleek bij twaalf gemeentes de koppeling van het betreffende CMS met DigiD zodanig te zijn opgebouwd dat er een potentieel risico bestond dat DigiD misbruikt kon worden. De kwetsbaarheid was volgens de softwareleverancier van het CMS binnen vierentwintig uur na ontdekking gedicht door middel van een patch. De softwareleverancier heeft de betrokken gemeenten geïnformeerd. Uit een onderzoek van een gerenommeerd beveiligingsbureau en de softwareleverancier zelf, bleek dat er geen aanleiding was om aan te nemen dat er gegevens in verkeerde handen zijn gevallen. Er zijn geen aanwijzingen dat er misbruik is gemaakt van de kwetsbaarheid. De namen van de twaalf gemeentes zijn niet bekend gemaakt door Logius, omdat het aan de betrokken organisaties zelf is om daar wel of geen mededelingen over te doen. Het betrof immers een kwetsbaarheid in een CMS dat door die organisaties zelf wordt gebruikt; er was geen lek in de beveiliging van DigiD zelf. Het beveiligingsniveau binnen de keten van DigiD is met de patch die de softwareleverancier beschikbaar heeft gesteld en heeft doorgevoerd in de specifieke versie van haar CMS, weer op orde.

Ik kan de leden van de CDA-fractie bevestigen dat in het conceptwetsvoorstel computercriminaliteit III geen afzonderlijke titel in het Wetboek van Strafrecht is opgenomen voor computerdelicten. In antwoord op een vraag van de leden van de PvdA-fractie heb ik hierboven reeds aangegeven waarom de introductie van een afzonderlijke titel voor computerdelicten niet voor de hand ligt. Graag verwijs ik deze leden kortheidshalve naar dat antwoord.

2. Hoofdlijnen wetsvoorstel

De leden van de VVD-fractie vroegen, althans zo begrijp ik hun vraag, in hoeverre bij de komende modernisering van het Wetboek van Strafvordering ook rekening wordt gehouden met een eventuele aparte titel voor computerdelicten in het Wetboek van Strafrecht.
Zoals hierboven in antwoord op een vraag van de leden van de PvdA-fractie reeds aan de orde kwam, ligt het niet in de rede om in het Wetboek van Strafrecht een aparte titel voor computerdelicten op te nemen. Kortheidshalve verwijs ik deze leden voor een toelichting graag naar het genoemde antwoord. Ten aanzien van het Wetboek van Strafvordering merk ik op dat het hierboven reeds genoemde wetsvoorstel computercriminaliteit III de noodzakelijke strafvorderlijke

bevoegdheden aan het Wetboek van Strafvordering toevoegt. Deze bepalingen zullen bij de modernisering van het Wetboek van Strafvordering worden overgeheveld naar het nieuwe wetboek en zullen daarbij een plaats krijgen in een gestructureerde en inzichtelijke ordening van de bevoegdheden.

De artikelen 350c en 350d WvSr, zo luidt mijn antwoord op de hierop betrekking hebbende vraag van de leden van de CDA-fractie, worden middels dit wetsvoorstel in artikel 67, eerste lid, onder b, van het Wetboek van Strafvordering opgenomen. Ik verwijs naar artikel II van het wetsvoorstel. De overige strafbepalingen die met dit wetsvoorstel worden gewijzigd (artikelen 138ab, 138b, 139c en 139d), zijn reeds opgenomen in artikel 67, eerste lid, onder b, van het Wetboek van Strafvordering.

De leden van de PVV-fractie lazen in de memorie van toelichting dat bestaande wettelijke bepalingen een ruimere bescherming bieden dan de richtlijn en dat Nederland, op artikel 9 van de richtlijn na, reeds voldoet aan hetgeen waartoe de richtlijn verplicht. Zij stelden enkele vragen over de meerwaarde van de implementatiewetgeving voor Nederland.
Ik antwoord op deze vragen dat, omdat computercriminaliteit naar zijn aard veelal grensoverschrijdend is en grensoverschrijdende gevolgen heeft, het noodzakelijk en wenselijk is om een gezamenlijke Europese aanpak te ontwikkelen. De richtlijn draagt bij aan het voorkomen van «safe havens». Doordat bepaalde strafbare feiten in alle lidstaten strafbaar moeten worden gesteld en minimaal met een bepaalde straf moeten zijn bedreigd, kan worden voorkomen dat personen (via computers) in landen waar bepaalde feiten niet strafbaar zouden zijn gesteld of met een lage straf zouden worden bedreigd, computercriminaliteit ten aanzien van de Nederlandse overheid, Nederlandse bedrijven en Nederlandse burgers zouden kunnen plegen. Daarnaast is het vanwege het grensoverschrijdende karakter veelal niet mogelijk om een verdachte (alleen) in Nederland op te sporen en te vervolgen, terwijl de gevolgen wel in Nederland neerslaan en gestopt moeten worden. Ook daarom is een gezamenlijke Europese aanpak van groot belang.
Voor de Nederlandse wetgeving heeft de richtlijn tot gevolg dat de straffen voor een aantal computerdelicten worden verhoogd en dat er bepaalde strafverzwarende omstandigheden aan de strafbepalingen worden toegevoegd. Het gaat bij de strafverzwarende omstandigheden om een strafverhoging wanneer gebruik wordt gemaakt van een zogenoemd «botnet», wanneer het feit ernstige schade tot gevolg heeft en wanneer het strafbare feit is gepleegd tegen een informatiesysteem (geautomatiseerd werk) van een vitale infrastructuur.
Uit de impact assessment die de Europese Commissie ten behoeve van de richtlijn heeft gemaakt, blijkt dat als gevolg van het samenstel van de voorgestelde maatregelen, lidstaten beter voorbereid zijn op grootscheepse aanvallen op informatiesystemen, en de veiligheid en de veerkracht van de kritische infrastructuur voor informatietechnologie en communicatie zullen toenemen. Een cijfermatige onderbouwing van hoeveel computerdelicten kunnen worden voorkomen of succesvol kunnen worden vervolgd als gevolg van deze richtlijn, is niet te geven. Door de in de richtlijn opgenomen verplichting om statistische gegevens te verzamelen en te verstrekken, kan op termijn meer inzicht worden gegeven in het aantal gepleegde computerdelicten en het aantal daarvoor vervolgde en veroordeelde personen.
Voor het antwoord op de vraag van deze leden of een subsidiariteits- en proportionaliteitstoets is uitgevoerd bij dit wetsvoorstel, merk ik op dat dit wetsvoorstel noodzakelijk is om te kunnen voldoen aan de verplichtingen uit de richtlijn. In het wetsvoorstel worden, conform de gebruikelijke praktijk, enkel wijzigingen aangebracht die voortvloeien uit de richtlijn.
Ten aanzien van de richtlijn heeft Nederland zowel de subsidiariteit als de

proportionaliteit van het voorstel positief beoordeeld. Ik verwijs ook naar het destijds opgestelde BNC-fiche (*Kamerstukken II* 2010/11, 22 112, nr. 1082). Omdat computercriminaliteit met name een grensoverschrijdend probleem is, kan dit fenomeen beter – door middel van in een richtlijn op te nemen minimumregels – op het niveau van de Europese Unie worden aangepakt dan door de lidstaten afzonderlijk. De richtlijn bevat minimumregels die niet verder gaan dan nodig is om de aan die richtlijn ten grondslag liggende doelen te bereiken. Het voorstel kan bijdragen aan onderlinge samenwerking tussen de lidstaten bij de aanpak van computercriminaliteit die, zoals gezegd, veelal een grensoverschrijdende dimensie heeft.

Tot slot vroegen de leden van deze fractie hoe ervoor gezorgd gaat worden dat computercriminaliteit daadwerkelijk beter opgespoord en harder bestraft gaat worden.

Zoals hierboven op vragen van de leden van de CDA-fractie al aan de orde kwam, is het aantal fte bij het THTC en het openbaar ministerie in de afgelopen jaren uitgebreid. In 2015 is het THTC op sterkte en zal het team, zoals aangegeven in de Veiligheidsagenda 2015–2018, de high tech crime-zaken oppakken, conform het huidige toewijzingskader. De overige zaken worden bij de regionale eenheden van de politie uitgevoerd. Daarbij kan het ook om relatief complexe zaken gaan. In het Inrichtingsplan van de Nationale Politie is een capaciteit voor digitale expertise en cybercrime van 743 fte voorzien. De intensivering van de bestrijding van computercriminaliteit leidt tot een toename van het totaal aantal onderzoeken naar deze vorm van criminaliteit van 200 in 2015 naar 360 in 2018. Door de formulering van doelstellingen en de voornoemde uitbreidingen is voorzien in capaciteit en prioriteit voor de opsporing en vervolging van computercriminaliteit. Met de inwerkingtreding van dit wetsvoorstel worden enkele strafmaten verhoogd en strafverzwarende omstandigheden geïntroduceerd. Dat zal gevolgen hebben voor de strafeisen die worden geformuleerd door het openbaar ministerie.

3. Inhoud richtlijn en wijze van implementatie

De leden van de VVD-fractie vroegen naar artikel 7 van de richtlijn, dat onder andere ziet op het tegengaan van het vervaardigen van kwaadaardige software. Zij vroegen of en hoe het vervaardigen van programma's – die zowel goedschiks als kwaadschiks kunnen worden gebruikt – voor zover deze programma's nodig zijn voor een goedschikse inzet, door de politie en de veiligheidsdiensten mogelijk blijft.

Artikel 7 van de richtlijn verplicht de lidstaten tot het treffen van de nodige maatregelen om onder meer strafbaar te stellen het vervaardigen van een computerprogramma dat hoofdzakelijk is ontworpen of geschikt is gemaakt voor het plegen van de in de artikelen 3 tot en met 6 van de richtlijn bedoelde strafbare feiten, dan wel een computerwachtwoord, toegangscode of soortgelijke gegevens waarmee toegang kan worden gekregen tot een informatiesysteem of een deel daarvan (hierna: software). Een vereiste voor strafbaarheid is volgens artikel 7 van de richtlijn dat een en ander opzettelijk geschiedt en met het oogmerk om de instrumenten te gebruiken voor het plegen van de in de artikelen 3 tot en met 6 van de richtlijn bedoelde feiten. De in die artikelen genoemde feiten stellen voor strafbaarheid steeds de eis van onrechtmatigheid. Voor zover er dus rechtmatig wordt gehandeld – bijvoorbeeld op basis van een bevoegdheid op grond van het Wetboek van Strafvordering of de Wet op de inlichtingen- en veiligheidsdiensten – is er geen sprake van een strafbaar feit als bedoeld in de artikelen 3 tot en met 6 van de richtlijn. Het vervaardigen van software met het oog op de rechtmatige inzet door de veiligheidsdiensten en de politie, valt dan ook niet onder het bereik van artikel 7 van de richtlijn. Ik verwijs ook naar overweging 16 bij de richtlijn waarin staat: »Aangezien strafbaarstelling moet worden voorkomen

wanneer dergelijke instrumenten worden vervaardigd en in de handel worden gebracht voor legitieme doeleinden, zoals het testen van de betrouwbaarheid van informatietechnologieproducten of de beveiliging van informatiesystemen, moet er, naast het algemene vereiste van opzet, ook een bijzonder oogmerk zijn vereist om deze hulpmiddelen te gebruiken voor het plegen van de in deze richtlijn opgesomde strafbare feiten.» Het blijft derhalve, zo beantwoord ik een volgende vraag van deze leden, mogelijk om rechtmatig dergelijke programma's te produceren, ook voor particulieren.
Een bepaling als artikel 7 van de richtlijn, gold al in de Nederlandse wetgeving in verband met de implementatie van artikel 6, eerste lid, van het Cybercrimeverdrag. In de Nederlandse strafwetgeving is bovenstaande reeds verdisconteerd doordat voor strafbaarheid steeds de eis van wederrechtelijkheid geldt en doordat in artikel 139d WvSr en artikel 161sexies, tweede lid, WvSr (dat met dit wetsvoorstel zal worden verplaatst naar het voorgestelde artikel 350d WvSr) een bijzonder oogmerk is opgenomen.

Voor het antwoord op hun vraag of de spionagesoftware van de politie onder de strafbaarstelling valt van artikel 7, onder a, van de richtlijn dan wel (het daaraan gelijkluidende) artikel 6, eerste lid, van het Cybercrimeverdrag, verwijs ik de leden van de SP-fractie kortheidshalve graag naar het antwoord dat ik hierboven heb gegeven op een soortgelijke vraag van de leden van de VVD-fractie.
Artikel 7 van de richtlijn komt overeen met artikel 6, eerste lid, van het Cybercrimeverdrag. De term «hoofdzakelijk», zo luidt mijn antwoord op de vraag van de leden van de SP-fractie naar de betekenis van die term, heeft dan ook dezelfde betekenis als in dat verdrag. Voorwerp van het strafrechtelijk verbod zijn die middelen die hoofdzakelijk voor het begaan van de genoemde delicten zijn ontworpen of geschikt gemaakt. Zoals hierboven al aan de orde kwam, moet voorkomen worden dat software die wordt vervaardigd en op de markt wordt gebracht voor legitieme doeleinden, onder de strafbaarstelling valt. Uit de inrichting en de eigenschappen van het middel dient te blijken dat het door de producent (ook) bedoeld is om de genoemde delicten te begaan. Er is niet gekozen voor de term «uitsluitend» of «specifiek», omdat daardoor onoverkomelijke bewijsproblemen zouden ontstaan. De verdachte zou om in een dergelijk geval vrijgesproken te worden, slechts behoeven aan te tonen dat het middel ook voor enig ander gebruik geschikt is. De term «hoofdzakelijk» sluit niet uit dat ander, al dan niet legitiem, gebruik mogelijk is, maar impliceert dat zodanig gebruik als ondergeschikt moet worden beschouwd ten aanzien van de naar objectieve maatstaven vast te stellen gebruiksmogelijkheden, namelijk als hulpmiddel tot het begaan van de in artikel 7 van de richtlijn genoemde strafbare feiten. Aldus ook over de term «hoofdzakelijk» de memorie van toelichting bij het wetsvoorstel tot goedkeuring van het Cybercrimeverdrag (*Kamerstukken II* 2004/05, 30 036, nr. 3, p. 19) en paragraaf 73 van het explanatory memorandum bij het Cybercrimeverdrag.
Deze leden vroegen tot slot waarom in de richtlijn is gekozen voor een maximumstraf van twee jaar en waarom Nederland niet zelf voor die termijn heeft gekozen bij de totstandkoming van nationale wetgeving. Anders dan de richtlijn, voorzag het Cybercrimeverdrag niet in minimale maximumstraffen. Het kaderbesluit zag voor een beperkt aantal gevallen in een – per saldo – minimale maximumstraf van één jaar. Bij het bepalen van het strafmaximum van de verschillende delicten, is destijds gekozen voor aansluiting bij de strafmaxima van aanverwante delicten. Zo is bij computervredebreuk (artikel 138ab Sr) gekozen voor dezelfde maximale gevangenisstraf als voor huisvredebreuk (artikel 138 Sr), te weten één jaar. Bij de strafbaarstelling van vernieling van computergegevens (artikel 350a Sr) is gekozen voor een strafmaximum van twee jaar, dezelfde

maximale straf als die geldt voor de vernieling van goederen (artikel 350 Sr). Voor een deel van de delicten uit de richtlijn, geldt de maximumstraf van twee jaar in Nederland dus al. Nederland heeft zich tijdens de onderhandelingen over de richtlijn ingespannen voor minimale maximumstraffen van twee jaar. Een minimale maximumstraf draagt bij aan het voorkomen van «safe havens». De verhoging van de strafmaxima naar twee jaar is meer in overeenstemming met de toegenomen ernst van aanvallen op informatiesystemen in het huidige tijdsgewricht. Vgl. onder meer *Kamerstukken I* 2010/11, 32 317, AJ, p. 6. In deze minimale maximumstraffen is in mijn ogen een belangrijke meerwaarde gelegen van de richtlijn ten opzichte van het kaderbesluit.

De leden van de SP-fractie vroegen wanneer sprake is van «ernstige schade». Het begrip «ernstige schade» is in de richtlijn noch dit wetsvoorstel nader gedefinieerd. Of een ontstane schade als ernstig kan worden aangemerkt, is mede afhankelijk van de concrete omstandigheden van het geval. Het ligt daarom voor de hand dat de rechter in het concrete geval een afweging maakt in hoeverre de schade als ernstig is aan te merken. Voorbeelden van gevallen waarin sprake kan zijn van ernstige schade is wanneer systeemdiensten van (groot) openbaar nut worden ontregeld, wanneer er aanzienlijke financiële schade is geleden of wanneer persoonsgegevens of gevoelige informatie worden gewist of openbaar gemaakt (vgl. overweging 5 van de richtlijn).
Voor het antwoord op de vraag van deze leden wat het doel is van het registreren van statistische gegevens, verwijs ik hen kortheidshalve graag naar mijn hierboven gegeven antwoord op vragen van de leden van de PvdA-fractie naar de statistische gegevens. Zoals ik op die plaats reeds heb aangegeven is het doel van het verzamelen van de gegevens om een vollediger beeld te krijgen van de problematiek van computercriminaliteit en netwerk- en informatiebeveiliging op het niveau van de Unie en dat er een doeltreffender reactie kan worden geformuleerd. Het verstrekken van informatie kan een beter inzicht bevorderen in huidige en toekomstige bedreigingen, en aldus bijdragen tot een meer passende en gerichte besluitvorming over het bestrijden en voorkomen van aanvallen op informatiesystemen (vgl. overweging 24 van de richtlijn).
Artikel 14 van de richtlijn verplicht ertoe om ten minste de reeds beschikbare gegevens over het aantal strafbare feiten en het aantal personen dat is vervolgd en veroordeeld, te registreren. Het gaat daarbij, zo beantwoord ik een vraag daarnaar van deze leden, om cijfers over zowel het aantal vervolgingen als het aantal veroordelingen.
De hierboven al genoemde 24/7-contactfunctie, zo kan ik de leden van de SP-fractie bevestigen, werkt naar behoren op de wijze zoals was voorzien bij de inrichting daarvan. Het contactpunt, dat is ondergebracht bij het THTC, staat in direct contact met de landelijke officier van justitie op het gebied van computercriminaliteit. Het openbaar ministerie beslist in een geval van een verzoek om rechtshulp of het verzoek wordt ingewilligd en door wie het wordt uitgevoerd, het THTC of een regionale eenheid van de politie. Alle rechtshulpverzoeken worden geregistreerd in het systeem Luris. In 2012 werden er 1111 verzoeken geregistreerd, in 2013 1270. Het gaat hier om een wat ruimere kring van verzoeken dan waarop de richtlijn betrekking heeft. Ook kinderpornografie is bijvoorbeeld meegenomen in de cijfers. Op basis van het Cybercrimeverdrag geldt op dit moment nog geen minimale responstijd, zo beantwoord ik een hierop betrekking hebbende vraag van deze leden. De richtlijn, die met dit wetsvoorstel wordt geïmplementeerd, bevat wel een minimale responstijd; artikel 13, eerste lid, van de richtlijn bevat de verplichting voor de lidstaten om ervoor te zorgen dat in geval van dringende verzoeken tot bijstand binnen maximaal acht uur na ontvangst ten minste kan worden aangegeven of het verzoek om bijstand zal worden ingewilligd, alsmede de vorm waarin en het tijdstip waarop dit naar verwachting zal gebeuren. In beginsel is het

THTC in staat om binnen vierentwintig uur na binnenkomst van een verzoek acties te ondernemen dan wel het verzoekende land te berichten hoe en op welke termijn actie kan worden ondernomen. Aan het vereiste om bij dringende verzoeken binnen acht uur te laten weten of het verzoek wordt ingewilligd, zal kunnen worden voldaan. In de praktijk volgen op de acties vaak nog nieuwe vragen. Het doel is om het volledige verzoek in twee weken volledig te hebben afgehandeld.

4. Financiële consequenties

De eventuele (beperkte) financiële gevolgen van dit wetsvoorstel, zo beantwoord ik een vraag van de leden van de PVV-fractie, worden binnen de begrotingen van de uitvoerende diensten opgevangen.

De Minister van Veiligheid en Justitie,
I.W. Opstelten